OL

Information Communication Technology (ICT)

Acceptable Use Policy for: DMAT, Durrington High School & The Laurels Primary School

2026-2027

Compiled/ Reviewed and Updated	**Author:** Matt Angell	**Date:** June 2026
Approval By: CEO/Exec Team – P Montalto	**Date:** 13th July 2026	**Review Date:** **July 2027**

CONTENTS

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

Introduction and Policy Principles

Introduction

IT is provided to support and improve the teaching, learning and well-being in DMAT schools as well as ensuring the smooth operation of the wider administrative and financial systems of the Trust.

This policy sets out the Trust's expectations in relation to the appropriate use of any computer or other electronic device that is owned/provided by the Trust or personally owned and used on a Trust network(s).

The policy provides additional advice and guidance to users covering the safe use of IT and social media. The acceptable use of ICT will be covered during the induction process for users. The policy, for reference, will remain open to access by Trust users on the network. Ongoing training, support and advice will be provided by the Trust as well as updates to this policy as/when deemed necessary. Training can/will also be provided at the specific request of an individual/group of staff. We encourage all users to be proactive in asking for advice and support so as not to place themselves or the Trust at risk.

This policy forms part of the terms and conditions of all employee contracts of employment and may be amended at any time. A breach of this policy is likely to result in disciplinary action and, in the event of illegal activity, a referral to external agencies.

Scope and purpose

The purpose of this policy is to ensure that all users are clear on the Trust's rules and personal obligations when using IT, and to protect individuals and wider schools/organisations that are part of the Trust from risk. In addition, it covers employee- specific wider use of social media.

Key definitions

Users: encompasses a broad group of individuals some of whom may have no direct contract of employment but may have reason to visit a Trust site and/or use the Trust provided IT facilities as part of their visit. "Users" include groups such as:

- Staff
- Members
- Trustees
- Governors

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

- Volunteers
- Trainee teachers
- Casual supply staff
- Consultants
- Adults make one off or periodic visits to a Trust school(s) for training and/or monitoring purposes
- Contractors and third party employed cleaning and catering staff

Trust networks/IT facilities: this includes* all trust/school maintained and commissioned:

- Electronic hardware
- Cloud Services
- Software & Applications
- Communication systems including, but not limited to
    - Email
    - Telephone
    - mobile devices & handheld radios
- Data storage (on and off site)
- Remote access
- Network services including, but not limited to
    - The hardwired network
    - Wireless network

IT Support provider: this includes the central DMAT IT Services Team, onsite technician or contracted IT support provider.

Ensuring IT is used in an appropriate way is the responsibility of every user. This also applies to Trust equipment and personal use of social media which may be on or off Trust/school environments.

Policy breaches

Users may be required to act if it is deemed that they have breached this policy (examples being removing internet postings or images). Failure to comply with such a request may in itself result in disciplinary action which would be managed through the disciplinary procedure.

Users, if in breach of this policy, may be barred from use of Trust IT facilities. If users are found in serious breach of this policy the Trust may consider this to be gross misconduct which could lead to dismissal.

If a school leader determines it necessary, to investigate a breach of this policy the relevant user will be required to share relevant password and login details to school accounts. Users who break the law when using Trust IT will be referred to the police.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

If you reasonably believe that any adult user has breached this policy, you should report it without delay to the Co/ Headteacher.

Trust personnel responsible for implementing the policy

The Local Committee of each school has overall responsibility for the effective operation of this policy, however day-to-day responsibility for its operation is delegated to the Co-Headteacher / Headteacher on each school site.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with each school's Headteacher/Co-Headteacher, the CEO of the Trust, Director of Operations and, if the school has one, the designated member of the SLT.

All users have a specific responsibility to operate within the boundaries of this policy, ensuring that all adults fully understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it.

For further clarification about any part of this policy, users should be pre-emptive in speaking to a member of senior staff within the school/Trust or the Director of Operations who will provide further advice/guidance.

Any misuse of IT should be reported to the relevant senior leader or Director of Operations immediately.

Any breach of this policy may result in disciplinary action and the Trust reserves the right to involve wider agencies (such as the police) if there is the possibility that illegal activity has occurred.

Network & Usage monitoring

Durrington Multi Academy Trust and its schools utilise a number of network and usage monitoring systems across their networks. Access to these systems is restricted to key colleague and external contractors.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

The physical hardware, all electronically stored materials, information that has been printed and licensed software installed on all Trust IT systems remain the property of the Trust.

Users of Trust IT (hardware, software and networks) should have no expectation of privacy in relation to:

- storing or transmitting of any electronic communication (for example email)
- creation and/or saving of data in electronic files, documents or media
- the use of Trust telephone networks
- social media post conversations/messages/postings, and/or
- printing of information
- Accessing website and personal content via a Trust IT device

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT hardware, software and/or networks, including but not limited to social media postings and activities, to ensure that school policies are being complied with and for legitimate business purposes. Users consent to such monitoring by using Trust hardware/software and/or networks.

Monitoring includes, without limitation, the tracking, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages, communications, postings, log ins, recordings, and other uses of the systems, as well as keystroke capturing and other network monitoring technologies.

We may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

Users must not use Trust IT hardware, software, or networks for any matter that they wish to be kept private or confidential from the Trust. Under GDPR, documents and emails containing pupil names may need to be disclosed to third parties including parents/carers, pupils and/or external agencies such as the police.

Use of the internet

Durrington Multi Academy Trust utilises firewalls and content filtering across all school sites, to protect all IT users from harmful content. the use of filtering and restrictions on each school site must remain appropriate and proportionate. The use of internet filtering must not affect the day-to-day operation of the school or be a barrier to teaching and learning. The day-to-day operation of the schools filtering system is the

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

responsibility of the schools' IT Support Provider, however the overall responsibility for managing the effectiveness of its implementation is with each school's DSL.

Internet usage (general)

Users are required to:

- Check their work emails at least twice a day (on workdays) as email is used to communicate important messages to both staff and pupils regularly.
- Use their own, and only their own, login credentials (username and password) to access the internet and any other software they have reason to use as part of their role (for example Arbor).
- Not give out personal information about a pupil or another employee over the internet without being sure that the request is valid, and they have the permission to do so. For questions in relation to GDPR seek guidance directly from your local designated data controller.
- Avoid visiting websites or downloading content that might be considered inappropriate/illegal or potentially harmful to the Trust, pupils, other staff, or the network. Such sites include*
    - Those with proxies
    - Dating sites
    - Hacking/hacking related sites
    - Sites containing or linking to pornographic content
    - Sites relating to non-educational gaming
    - Sites relating to gambling

Durrington Multi Academy Trust utilises firewalls and internet filtering services to store internet history on all devices connected to the trust's networks. Users should be aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

Users should:

- Not publish or store copyrighted material on the school network or wider internet.
- Report any unsuitable/inappropriate/illegal content found on Trust networks/hardware of software to the school's IT support provider immediately

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

- Alert their school's IT support provider and a member of the senior leadership team if they:
    - receive any messages/attachments that make them feel uncomfortable or that you believe to be unsuitable/illegal.
    - view content that makes them feel uncomfortable, or they think is unsuitable (even by mistake).
- Remember that everything users do on our Trust network will be subject to monitoring
- Not, at any time, use the Internet/network in a way that may interfere with the efficient running of the school (this includes storing excessive amounts of data-heavy files)

Staff utilising remote access services are required to use a device with appropriate permissions and security (for example a password protected computer and home network) in place before initiating this use (for guidance on what is required, speak to a member the IT support provider).

Users are also advised not to:

- Give out personal information such as their address, telephone number or mobile number over the internet without being sure that the receiver is from a reputable source.

The use of Twitter, YouTube, and Google images (as well as other approved educational sites) has been opened to all users for use as teaching, learning and support resources should staff wish to use them. If users choose to open/use these or similar websites with a pupil/s as part of their work/role the Trust expects them to follow the following expectations as set out below.

Users, when opting to use Trust ICT (e.g. using guest Wi-Fi when on site) are required not to*:

- use ICT in any way that could damage the network (physically or virtually) - access, download or publishing any material that is illegal (users should be aware that by accessing the network their personal files and activity will be subject to monitoring)
- use the network in a way that has a negative impact on other users/users (e.g., by downloading large files*)

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

- access any information that cannot be seen to directly relate to their reason for using the network/being on site (for example* not accessing pupil details unless there is a specific reason to do so).

If users have any questions about the use of Trust ICT these should be referred to your schools IT Support provider.

Failure to follow these expectations is likely to result in a user being banned from future use. Where there is the possibility that a user's behaviour has broken the law, the Trust reserves the right to contact all necessary outside agencies.

Guidance specific to the use of the internet in the classroom/in front of pupils

This guidance must be followed every time staff show material from the Internet to a class/group of pupil/pupils.

- Prior to showing the material the employee must review, in full, the intended content and check that all the information intended to be shown is suitable for the audience it is being shown to.
- Users must only show age-appropriate material to the pupil(s). If material has no age rating, then no clip will be shown that contains swearing, any form of racial, gender or other type of harassment/hate content, inappropriate sexual content, nudity, or anything that could reasonably be considered to cause offense to the watchers.
- Users are expected to check any material that could be considered "borderline" with an appropriate curriculum or a member of SLT prior to showing it to the class.

Use of school email

Trust provided email systems

Before sending an email, users should check it carefully and consider whether the content is appropriate, treating emails like you would any other form of formal written communication. When sending emails internally relating to a pupil(s), staff should use the pupil's initials and year/class in replacement to full names.

Although the email system is provided for business purposes, we understand that users may, on occasion, need to send or receive personal emails using their work email

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

address. This should be kept to a minimum and should not affect or be to the detriment of you carrying out your role effectively. If sending personal emails from a work email account, users should show the same care in terms of content as when sending work-related emails.

Users must never:

- Open an attachment on an unsolicited email from an unknown email address without first checking with their IT support provider. Attachments could contain viruses or inappropriate/illegal content.
- Send personalised data/information about any other stakeholder (e.g., pupil(s) and/or parent/carer) to any person(s) who are not employed by the Trust other than:
    - Data that is necessary e.g., safeguarding documentation, that requested by the police*
    - Data which you have the express permission e.g., in the case of a pupil from the pupil themselves or from their parent/carer to share with a named external professional

All data/information sent externally in this way must be in encrypted format via Egress (or similar secure) system

- Use email to send or forward messages which are defamatory, obscene, or otherwise inappropriate. This will be considered under the disciplinary procedure.
- Use the school email system to make personal or offensive comments about pupils, users, parents, carers, or any other person(s) that could cause harm or offence
- Contact a pupil or pupils on their personal email addresses, additionally, staff must ensure that all email communication is kept within appropriate hours (generally between 7.30am and 8pm on weekdays)

If an employee receives an abusive, obscene, defamatory or any other form of concerning email or wider social media communication you should alert a member of the senior leadership team. In the case of an email, you suspect may contain malicious content e.g., viruses, unsolicited attachments or similar these should be alert a member of your school's IT support provider for investigation.

Trust advice is to use the "rule of 2" when communicating using email. This means users seeking to speak to or meet with the other person (parent/carer/ colleague/external professional) after two email communications have been exchanged on the same topic/issue. Adopting this approach will reduce the potential for one or both parties misinterpreting information.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

Personal email accounts

Users are strongly encouraged not to use Trust hardware/software of networks for the access/sending/receiving of personal emails. Logging into personal accounts/using Trust networks/hardware/software makes the contents of personal email public and subject to monitoring.

Mobile Devices

The use of mobile tablets/laptops or other mobile or portable devices

A variety of mobile devices are provided by the Trust with the purpose of enhancing teaching and learning and making users' work more efficient. These include:

- Laptops and tablet computers and iPads*
- Cameras (still and video)*
- Mobile phones (principally used for safeguarding on trips)*
- As well as a range of other subject area/specific items.

The following expectations apply to all users who use mobile devices provided by the Trust/school:

- Access to our wireless network must be approved by the school's IT support provider.
- Users must ensure that mobile devices that are on loan to them (from the school/Trust) and have the facility to be password protected and are secured with a password/code. This is particularly important if you are taking the mobile device off site.
- Users are expected to ensure that all Trust owned devices in their care are securely locked away when they are not being used. You must not leave your mobile device in an unsafe place, for example in your car or unlocked classroom. Furthermore, devices are expected to be kept in the cases provided so as to reduce the risk of damage.
- Should a user wish to take a Trust/school-owned mobile device off site it is their responsibility (in advance of doing this) to:
    a) Gain permission from the Headteacher, a member of SLT or Director of Operations and sign a request to take IT offsite form as a record of receiving and taking responsibility for the device.
    b) Ensure they have appropriate insurance in place so as to cover damage or theft of the device when off site
    c) Ensure that when taken off site the device is stored in a safe and secure way and that only the user uses the device.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

d) Ensure the device remains password protected (where the device has the facility for this to be set up)

- In the event of a Trust/school-owned device being damaged, the Headteacher, a member or SLT or Director of Operations should be notified immediately.
- Users are made aware that school/Trust owned mobile devices are monitored (including historical use e.g., browser history). It is the user's employee's responsibility to ensure that only appropriate content (as set out in this policy) is stored on the device. Failure to do so could result in a breach of this, or other, policies/laws.

The use of personal mobile devices on the network/in schools

Personal mobile devices may be used on the Trust's network(s) but are required (as compatible/applicable) to have up-to-date anti-virus installed before being connected to the network. It is the responsibility of the user to get this checked by the school's IT support provider.

Users are expected not to use mobile phones in front of pupils (i.e., when delivering a lesson/in a classroom with pupils or in public spaces within the school).

It is never appropriate to use personal imaging or recording devices (including phone cameras) to take pictures/record audio of pupils unless it is related to school activities e.g a sports/arts event.

The Trust reserves the right to disable access to the wireless network for any user at any time.

Specific guidance on the recording (still images, video, sound clips) of pupils

It is acceptable to record images or video of pupils for legitimate school aims which could include:

- The displaying of excellent pieces of work
- Coaching (pupils and/or staff) for improved performance
- Publicity in advance or and after events
- In-school displays

However, the following rules apply to a user recording the image/video:

- The user must let any pupil/person being photographed or videoed know whether or not their image will be retained for further use,
- The user must only use Trust/school devices (never personal devices including personal storage devices such as memory sticks) to record images/video on.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

- At no time must any images/video storage device (personal or Trust owned) be taken or used in any location (on or off site) where pupils or other users are changing clothing or could be in any state of undress (e.g., toilets. changing rooms, dressing rooms)
- The user, after recording the images, ensure they are moved and securely stored and be clear about the reason for their storage. Once the videos/images are no longer needed it is the user who recorded the image's responsibility to delete these from the Trust's network/devices.
- Personal data processed for any purpose should not be kept for longer than is necessary for that purpose. Users must not take images of pupils without their knowledge or approval.
- The user using the images/video is responsible for checking the permissions list (for both users and pupils) before the use of the image/video.

Social Media

Introduction

It is recognised that social media in all its forms, can be of use, both as an educational and communication tool. However, users' use of social media can pose a risk of others in misunderstanding the intent behind online communications and/or the blurring of professional boundaries between children and young people and/or their parents or carers.

A user could, if they were to use social media in an inappropriate way or with a lack of proper care:

- share confidential information
- cause damage to their own or another professionals' reputation
- cause reputational damage to the Trust/individual school they work for, and/or
- jeopardise the trust's/school's compliance with its legal obligations.

These risks could also be the case during non-school hours.

The Trust has the following guidelines which all users are expected to follow in relation to their own use of social media. The guidelines apply whether social media is being used for business or personal reasons, whether during working hours or otherwise, regardless of whether the social media is accessed using Trust ICT facilities or personally owned devices.

The following sections of the policy provide staff with guidelines and recommendations for using social media responsibly and safely and to protect Trust users.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

Communication with individuals

- Users should exercise caution when using social media.
- Users must block unwanted communications from pupils. In the (rare case) of offensive or harassing communications being sent to users these should be sent to a member of SLT before blocking.
- Users are personally responsible for what they communicate on social media.
- Users should never knowingly communicate with a pupil or pupils including ex-pupils up to the age of 21 via social media* or via personal email accounts/personal mobile phones or similar.
- Any communication with pupils **must be** through the school network/a school device so this can be appropriately monitored. If there is a need to communicate directly with a pupil or pupils, this should only be conducted through our usual channels e.g. school email address to school email address or by a phone call home.
- At no point should personal/private messages ever be sent to a pupil or pupils via social media by users.
- Communication, if it is appropriate/necessary, should only ever be related to school business. A school may on occasion use professional/school software to contact older pupils for safeguarding or educational reasons. e.g., to communicate up to date information regarding examinations

*(*the only exception to this is when general broadcast information is posted on school named/branded social media streams)*

Specific guidelines in relation to employee's personal use of social media

- All users should ensure that security settings on their social media accounts are set to the highest level of privacy. This is for their own protection. The DMAT IT Services team are available and willing to offer advice and support as necessary to users.
- If an employee decides to disclose their affiliation with DMAT and/or their school, they must also state that their views do not represent those of the employer. For example: "views/comments/postings are personal and in no way

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

representative of the views of my employer". Users should also ensure that their profile and any content posted are consistent with the professional image presented to pupils and colleagues.

- Users should avoid social media communications that might be misconstrued in a way that could damage school/Trust reputation, even indirectly.

- Users should make it clear in social media postings that they are speaking on their own behalf e.g., writing in the first person and use a personal e-mail address when communicating via social media.

- Staff are personally responsible for what they communicate on social media, remembering that what is published might be available to be read by the masses including the school itself, future employers and social acquaintances for a long time. Users should keep this in mind before posting content.

- Users should avoid posting comments about sensitive school-related topics. An example could be the school's/Trust's stance in relation to a specific issue or school performance. Even if it is made clear that views on such topics do not represent those of the school/Trust, comments could still damage reputation and/or be upsetting to those staff/pupils involved.

Posting about other individuals/the trust/schools

Staff must not post disparaging or defamatory statements about the Trust's:

- Schools
- Employees
- Individuals or groups of pupils' and/or their parents/carers
- governors & trustees of schools/DMAT
- suppliers and vendors,
- any other stakeholder linked to the schools/Trust.

In addition to this, users should not post or share anything/including any viewpoints (personal to them or not) that could bring the Trust, Trust leaders/governors/trustees and/or users into disrepute or damage the wider reputation of the Trust or its schools.

Users should be aware that breaching the above guidelines may lead to disciplinary action being taken.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

Personal use of ICT systems, services, and facilities

Whilst the Trust does allow for limited personal use of the IT facilities, it is expected that personal use, wherever possible, is limited to non-working time e.g., at lunchtime, before/after normal working hours.

Examples of limited use would be responding briefly to an incoming personal e-mail or telephone call or to deal with a non-work-related emergency.

It is not acceptable for an employee to spend significant amounts of time making personal use of the internet, e-mail, communication equipment, etc.

The following guidance must be adhered to if an employee chooses to make personal use of Trust ICT systems/services and facilities.

The use of Trust IT:

- Must not interfere with your work, or the work of others it is not acceptable for an employee to use the internet or network software in a way that triggers multiple Securus software safeguarding reports

- Classroom based staff must not use ICT for personal purposes during lesson contact time or at any other time when they are responsible for the supervision of pupils.

The use of Trust IT should not:

- involve more than minimal amounts of working time;
- incur any significant expense to the Trust and/or tie up a significant number of resources (virtual or physical)
- involve storage of any personal information or files on any part of the IT network.
- involve the downloading or storage of any copyrighted material or material that is illegal
- involve the viewing of any material deemed inappropriate in a professional context
- involve the downloading or installing of any personal software onto the network or Trust devices
- lead to personal gain (financial or otherwise) for the member of staff.

Before undertaking personal use, users should ask themselves the following questions:

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

- Would the actions be considered unacceptable if viewed by a member of the public?
- Would leaders, auditors or others in similar positions call into question the cost effectiveness of use of work time or use of school/Trust IT networks/devices?
- Will personal use have a negative impact upon the work of colleagues (e.g., in terms of their motivation and morale)?
- Could personal use bring the Trust/schools directly or indirectly into disrepute?

Personal use should not be undertaken if the answer to any of these questions is yes.

Responsibility for ensuring that any personal use is acceptable rests with the individual.

Users should seek guidance from their line manager if they have any doubts concerning the acceptability of their personal use. If any doubt remains, then that form of personal use should not be undertaken.

Users should be aware that breaching the above guidelines may lead to disciplinary action being taken.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

Use of mobile storage devices

Mobile storage devices are defined as any piece of hardware that can store electronic material (files/media/video/images etc) and can be easily moved between devices in a "plug and play" type way. This includes USB sticks and external hard drives.

The Trust/schools provide a range of remote access facilities as well as portable devices that are all password protected to support users in their work. This service/hardware is provided to reduce the need for staff to save/transfer information onto/off mobile storage devices.

It is however recognised that some users wish to use mobile storage devices. If an employee makes the choice to use a mobile storage device the following guidelines must be followed:

- All storage devices must be password protected and/or encrypted
- Storage devices should be regularly virus checked so ensure that no malicious material is transferred onto the trust's network.
- Work related material on the storage device should be regularly backed up on the system to minimise the risk of loss.
- Storage devices should uniquely store work-related information to minimise the risk of sharing material with other audiences outside work.
- Storage devices should be secured to keys or similar values items to reduce the risk of loss.

Even with the latter security in place the Trust strongly advises staff to use the remote access provision as loss of personal data is likely to be viewed as a disciplinary offence as well as breaching GDPR compliance.

The use of mobile storage devices will continue to be reviewed in line with the rest of this policy, and the trust/individual schools reserve the right to change the policy at any time.

At no point, whether Trust owned or personal, should any "jailbroken" or "hacked" device be connected to the Trust network. If users require advice on how to protect data on mobile storage devices, they should contact a member of the ICT service team.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

Use of mobile storage devices

Moving of equipment

Hardware (including keyboards/mice/printers) should not be moved. It is acceptable to adjust computer settings for comfort and ease of use, but these must be adjusted back after use for the next user.

Usernames, passwords and logging on to the system

Users must not disclose login username and password to anyone unless directed to do so by a member of the senior leadership team for monitoring purposes or as stated earlier in this policy.

Any member of staff viewing or caught trying to gain access to another member of staff's accounts, files or data will be subject to disciplinary action.

Users will be required to change their password in accordance with the login prompts, ensuring that they create appropriate passwords as directed. Passwords should not be written down where they could be used by another individual.

Users, before leaving a computer are expected to log off and ensure the logging off procedure is complete before they leave. If moving away from a PC for a short period of time, they should use the windows + L command to lock the computer. Projectors are also expected to have been switched off when users leave.

Users must not use any hardware/software under the username/profile of another employee. This includes Arbor/email/the network.

Only software provided or approved by DMAT IT Services may be run on the computers. You are not permitted to import or download applications or games from the internet.

Remote access

Remote access is provided to users to create more flexibility in their work, should they wish to use this.

Expectations in relation to employee's use of remote access include:

- Only using Trust-provided hardware or password protected (secure) personal devices to access the network.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

- Ensuring that any device used to access the network has up-to-date anti-virus software installed, to protect both the device and the network from harm.
- Logging in and out using the agreed protocols. This includes it being the employee's personal responsibility to log out of software applications (e.g., Arbor) to allow fair access to others.
- Ensuring that remote access is undertaken in a private space/area/location and that non-users (for example family members*) do not view or access Trust ICT or information.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

Reporting concerns and policy compliance

Malfunctions or technical issues must be reported to the designated IT support team as soon as they are found via the specified contact details.

Suspected breaches to this policy should be reported to a member of the on-site SLT of each school who will take the lead in deciding any action that needs taking.

Users should be aware that this policy is part of a wider range of policies and support documents that users are expected to adhere to in order to in order to fulfil their statutory and contractual obligations.

Examples of related policies/guidance include:

- Keeping Children Safe in Education
- The General Data Protection Regulations
- DMAT disciplinary policies
- DMAT Equality Diversity and Inclusion policy
- A range of wider UK laws
- Regulatory body laws e.g., copyright law

If an employee breaches this IT policy, they may also be in breach of policies and/or the law, and any action taken may not just be limited to that by DMAT. Users who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*

Associated documentation and policies

This policy should be read in conjunction with other Trust policies including*:

- The DMAT Safeguarding Principle
- DMAT Safeguarding and Child Protection Policy
- DMAT Data Protection Policy
- DMAT Disciplinary Procedure
- DMAT Privacy Notice for staff
- DMAT Privacy Notice for pupils and parents
- Individual employee's contract of employment

**Indicates lists are not exhaustive, but rather exemplars given to aid understanding in relation to the point made.*